REMARKS

The Office Action raised an issue under 35 U.S.C. §112 which is believed to be addressed by the currently amended claims.

The present invention represents a unique manner of addressing potential security issues in the transmission of information over a network and more specifically, in the environment of conventional encryption and decryption algorithms. The present invention recognizes the potential susceptibility of an attack from a third party based on the characteristics of the actual plaintext that is subject to encryption in a particular format where the content of the plaintext is traditionally considered not to be a significant factor in determining a difficulty of decryption.

The present invention has determined that selective portions of plaintext, which meets certain conditions would be more susceptible or subject to a decryption attack and accordingly, if such plaintext is detected, an adjustment in the encryption procedures can be implemented without requiring a drastic changing of encryption algorithms with the accompanying burden and computation costs.

Thus, the present invention can increase the difficulty of decryption, depending on the specific content of the plaintext, and can implement, for example, the changing of a key utilizing the encryption algorithm without necessitating a change in the encryption algorithm. Accordingly, a detecting part can receive blocks of plaintext and make a determination as to the susceptibility of an attack based on a characteristic of the plaintext and render a judgment as to whether the plaintext can continue to use the same encrypting key or whether a new encryption key should be implemented in the encryption process.

As can be appreciated, numerous different protocols and procedures have been utilized to encrypt and decrypt data that is forwarded over a network that is accessible to third parties. It is generally recognized that the degree in which data can be secured is basically a function of the amount of computation resources that must be devoted to the encryption procedure to withstand an attack. Thus, practical compromises are suggested in the prior art to maintain a sufficient level of security without significantly increasing the cost of the computational resources that must be devoted to the encryption and decryption protocol.

Needless to say, a number of scientists and computer engineers in this field have devoted significant resources to this problem and as more important commercial information is utilized over an open global network such as the Internet, more effort has been devoted to this particular problem.

Thus, the relative time period that this problem has been addressed in a relatively crowded field, should be taken into consideration in weighing the patentability of the present invention.

> "Thus when differences that may appear technologically minor nonetheless have a practical impact, particularly in a crowded field, the decision-maker must consider the obviousness of the new structure in this light."
>
> *Continental Can Co. USA Inc. v. Monsanto Co.*, 20 U.S.P.Q. 2d. 1746, 1752 (Fed. Cir. 1991).

The present inventors have taken a new tact in providing a higher level of security with minimal changes in computational resources by implementing a filter or detector to specifically analyze the content of the plaintext and to set a threshold value that is indicative of an increase of susceptibility of a decryption attack based on the particular content of the plaintext. The plaintext can be broken into appropriate blocks and a portion of the block can be separated. For example, any number of bits of the plaintext can be constituted arbitrarily as a fixed part while other portions of the block can be considered to be a variable part. A counter can count the number of inputted plaintext, each of which have the same value relating to the fixed part and this number can be maintained as a separate count. When that separate count exceeds a predetermined number or threshold, a detecting part can then output a detecting signal that indicates that the encrypted plaintext or ciphertext is becoming susceptible to a decryption attack.

Accordingly, preventive measures can be undertaken such as changing the key utilized by the particular encryption algorithm. Thus, by providing, for example in software code, this procedure for analyzing plaintext blocks and code, an improved encryption/decryption system can be implemented.

The Office Action contended that Claims 1, 2, 4, 6-8, 10 and 11 were held to be obvious over a combination of *Matyas, Jr. et al.* (U.S. Patent No. 5,978,124) in view of *Lynn et al.* (U.S. Patent No. 5,444,781).

The *Matyas, Jr. et al.* reference basically was an improvement of an earlier application by the same inventors by implementing an encryption procedure intended for relatively short blocks into encrypting a long plaintext block.

More specifically, this procedure was to be implemented in an asymmetric encryption system or public key encryption system where one key was utilized to encrypt the data while using another key to decrypt the same data, with the encryption key being made public and corresponding decryption keys being kept private and not shared with others. A decrypting private key cannot be derived from knowledge of a corresponding public key.

The *Matyas, Jr. et al.* patent recognized a problem in the implementation of an elliptic curve system that would typically have a relatively short key and encryption block sizes, for example in the order of 160 bits. In a public key distribution system, however, a problem can occur since the symmetric key is normally contained in a key block of a 512 bit block which is much longer than the elliptic curve encryption block.

The prior art had suggested that to ensure appropriate security, a number of masking rounds be utilized with an increase in computational expenses. The solution, as set forth in the Summary of the Invention in Column 3, Lines 28-36 is as follows:

> The present invention, on the other hand, recognizes the significance of a previously unrecognized factor, namely, the location of the portion of the masked block that is encrypted using an asymmetric algorithm.
>
> More particularly, in accordance with the present invention, the part of the masked input block that is encrypted is the masked part that was last used as an input to produce the last masking value. (underline added)

Thus, the solution was the particular manner in which the masked input block that is encrypted utilizes an input to produce the last masking value and thereby minimizes the number of required masking rounds, e.g., to three rounds. Thus, the invention in the prior art terms is limiting the number of masking rounds with a resulting decrease in computational expense.

The Office Action noted the utilization of the terminology "fixed bits" and more specifically cited a predetermined condition as taught in Column 4, Lines 19-23 as follows:

> Encryption procedure 100 has as its input a long plaintext block such as the key block 110 shown. In general, key block (or input block) 110 may consist of any desired data, such as a symmetric encryption key.

The Office Action does not note the following discussion, wherein the key block 110 is to contain a secret value, that is a secret DES key of a sufficient length to prevent exhaustion and to prevent a third party from inverting the masking procedure. This is taught in Column 4, Line 28, where at least 128 bits are selected as the value.

The Office Action also noted the teaching of Figure 5 which utilizes the terminology "fixed bits" as a portion of the key block 110. These fixed bits or predictable bits are used for non-malleability. That is, bits that can be used to verify that the key block has been properly recovered. Thus, the fixed bit is simply a first field 501 with fixed information to verify the recovery process. A second field 502 contains the symmetric encryption key or other secret information being conveyed to the recipient, while an optional third field contains a count from a counter that is incremented for each encryption of a plaintext block. This count field 503 simply ensures that the key block is unique for each encryption of a plaintext block. See Column 4, Lines 39-55.

As can be readily appreciated, the count is a value added to the actual plaintext key block and the key is actually incorporated into the key block. The fixed bits are not subject to a filtering or detection part that will monitor the plaintext per se to determine its susceptibility to a possible decryption attack after an encryption algorithm has encrypted the plaintext to ciphertext.

The improvement in *Matyas, Jr., et al.* is the masking procedure wherein the key block 110 is first masked as shown in Figure 1 or transformed into a masked key block 130 of the same size. The subportion of this masked key block is subsequently encrypted with an encryption key to generate an encrypted portion of a ciphertext block. The remaining portion of the ciphertext block can be simply taken from a corresponding portion of the masked block without encrypting it. Preferably, each bit in the masked key block is a function of each and every bit in the key block. See Figure 5, key block 110. No bit in the key block 110 can be determined unless every bit in the masked key block is known or available. See the description in Column 5, Lines 37-63.

Thus in summary, *Matyas, Jr., et al.* relates to the selection of a masked input block portion that is encrypted using an asymmetric algorithm. Needless to say, there is no recognition of the problem recognized by the present inventors nor any suggestion of the solution suggested by our present claims.

Thus, one highly relevant inquiry in making an evaluation under 35 U.S.C. §103 is "[t]he relationship between the problem which the inventor. . . was attempting to solve and the problem to which any prior art reference is directed." *Stanley Works v. McKinney Mfg. Co.*, 216 USPQ, 298, 304 (Del. D.C. 1981). Thus, in analyzing the prior art under Section 103 of the Act, we must clearly comprehend the problem addressed by the present inventors and that problem must be compared or contrasted, as the case may be, with the problems addressed by the prior art.

Pursuing further the "problem" analysis required under Section 103 of the U.S. Patent Act, the applicability of any reference against the claims of a pending U.S. patent application requires compliance with In re Gibbons, 100 U.S.P.Q. 298, where it is stated:

> In considering the questions of invention, it is <u>necessary</u> to determine whether or not the art relied upon contains <u>adequate direction</u> for the practice of the invention without resort to the involved application. (Emphasis added)

The *Lynn et al.* reference was purportedly cited to rectify the deficiency of the *Matyas, Jr. et al.* reference in not teaching a filtering or detecting part for outputting a detection signal when the accumulation of the counts from successive plaintexts reset a predetermined number and suggest the susceptibility of the ciphertext to being subject to a decryption attack.

The *Lynn et al.* reference also seeks a common desire to reduce the computational overhead associated with encrypting and decrypting digital data signals. It accomplishes this by ". . . selectively reusing, according to the desired level of security, a pseudorandom encoding sequence at the transmitter end and by storing and reusing pseudorandom decoding sequences at the receiver end." See Column 1, Lines 14-21. To accomplish this, the *Lynn et al.* reference suggests repeating the use of a key generated by a pseudorandom number (PN) generator and storing and reusing the PN sequences to thereby speed up the transmission rate of messages through the cryptosystem for a certain predetermined number of repetitive sequences, see Column 2, Lines 36-39.

Thus, the security level is reduced by utilizing the same key but only for a predetermined number of encryptions of messages. This is clearly set forth in Column 3, Lines 2-15 as follows:

> This temporal key is then used as an input to a pseudorandom number (PN) generator to produce a unique PN sequence of binary digits, for each new temporal key entered. The generated PN sequence is equal in length to the longest anticipated message fragment. The initialization vector together with its corresponding PN sequence is then stored in a cache and the PN sequence is iteratively reused, as determined by a counter, to encrypt one or more plaintext messages. The counter is initialized to a maximum count value whenever a new PN sequence is generated, and the counter tracks reuse of the PN sequence to encrypt the number of messages specified by the maximum count value.

The Office Action, in citing the utilization of a counter 21 in Column 5, Line 63 through Column 6, Line 10, is thus referring to counting the number of times the pseudorandom number key sequence has been utilized, not specifically counting specific bit values of the plaintext to suggest a condition that would render the overall ciphertext more susceptible to a third party decryption attack.

Thus, it is clear that neither the *Matyas, Jr., et al.* nor the *Lynn et al.* reference recognize the problem discovered by the present inventors and certainly is incapable of suggesting the solution as defined in our currently pending claims.

The Office Action fails the requirement to provide a specific reason that would teach the combination of elements in a fashion claimed by the patent at issue.

> Finally, to say that the missing step comes from the nature of the problem to be solved begs the question because the Board has failed to show that

> this problem had been previously identified anywhere in the prior art. *See In re Sponnable*, 405 F.2d 578, 585, 160 USPQ 237, 243 (CCPA 1969) ("[A] patentable invention may lie in the discovery of the source of a problem even though the remedy may be obvious once the source of the problem is identified."). See *In re Zurko*, 111 F.3d 887, 42 USPQ 2d 1476, 1479 (Fed. Cir. 1997)

More specifically, neither *Matyas Jr., et al.* nor the *Lynn et al.* teach the same invention as defined in our current claims and it becomes apparent that only the similarity of certain terminology, that is "fixed bits" and "counter" are being aggregated together without providing a proper context as defined in our claims. The counting of the number of times a pseudorandom key is repeated, and breaking a key block into a fixed portion of bits that must be located in a particular portion so that a series of masking rounds will help increase a level of security, does not address the analysis of the content of plaintext to determine susceptibility to decryption attack.

The newly drafted Claim 16 defines a plaintext detector system in analyzing potential susceptibility for blocks of plaintext, that are encrypted by an encryption algorithm, of being decrypted by an unauthorized party and upon such a detection, to increase the security of the encryption of such plaintext. Thus, a receiving unit receives a block of plaintext that is to be encrypted and subjects that plaintext to a preliminary detection procedure. A counter unit separates, from the block of plaintext, a predetermined bit stream that computes a value based on counting the predetermined bit stream. For example, by treating it as virtually continuing bits to represent a susceptibility standard of unauthorized decryption.

That is, if the plaintext represents a repetition based upon such a value in succeeding blocks, the encrypted plaintext or ciphertext becomes much more susceptible to an attack by an unauthorized third party. The detecting unit compares the computed value with a predetermined stored value and if the block of plaintext is less than the susceptibility standard of the predetermined stored value, a first signal is provided that basically can release the analyzed block of plaintext for encryption and transmission.

If, however, a block of plaintext is equal or greater than the susceptibility standard of a determined stored value, a second signal is provided that will change the manner of execution of the encrypted algorithm to prevent the repeatable sequence, such as changing the key of the encryption algorithm that is to be used on that block of plaintext.

As can be appreciated, the present invention deals with the specific content of the plaintext and based on such an analysis of the context and its susceptibility of providing repeated similarities in encrypted blocks, the encryption system can then be altered. Otherwise, the encryption system can continue to process the sequential plurality of plaintext blocks into ciphertext.

None of the references of record recognize or address the solution offered by the current claims.

The Office Action had rejected Claims 3, 14 and 15 over a combination of the *Matyas, Jr. et al.* and *Lynn et al.* reference when taken further in view of Pages 8-17 of the KASUMI Publication. The simple addition of a KASUMI type of encryption algorithm that deals with blocks of plaintext does not provide the missing claim elements from the hypothetical combination of *Matyas, Jr. et al.* and *Lynn et al.,* as now defined in our claims.

Claims 5, 9 and 12 were further rejected over *Matyas, Jr. et al.* and *Lynn et al.* in view of *Marchant* (U.S. Patent No. 6,094,486).

The same comments with regards to the combination of *Matyas, Jr. et al.* and *Lynn et al.* are equally applicable here. The *Marchant* reference is cited for the capability of changing an encryption algorithm and the Office Action contended that such a feature would permit an ability to change the encryption used for each string to provide a random choice of encryption algorithms on a randomly chosen length of string results. The Office Action does not recognize the computational cost of such a protocol, nor does it recognize the specific analysis of the content of the plaintext as the motivating feature of the present invention.

Finally, Claim 13 was rejected over *Matyas Jr., et al., Lynn et al.,* KASUMI Publication and *Marchant.*

In summary, this is a relatively congested field and numerous skilled parties have attempted to strike a proper balance between the level of encryption and decryption complexity with the cost and time of computational resources. Applicant has provided a unique recognition of a problem and has provided a specific solution not obvious.

> Finally, to say that the missing step comes from the nature of the problem to be solved begs the question because the Board has failed to show that this problem had been previously identified anywhere in the prior art. *See In re Sponnable*, 405 F.2d 578, 585, 160 USPQ 237, 243 (CCPA 1969) ("[A] patentable invention may lie in the discovery of the source of a problem even though the remedy may be obvious once the source of the problem is identified."). See *In re Zurko*, 111 F.3d 887, 42 USPQ 2d 1476, 1479 (Fed. Cir. 1997)

It is believed that the present application is now in condition for allowance and early notification of the same is requested.

If the Examiner believes a telephone interview will help further the prosecution of this case, the undersigned attorney would appreciate a telephone conference.

Very truly yours,

SNELL & WILMER L.L.P.

Joseph W. Price
Registration No. 25,124
600 Anton Boulevard, Suite 1400
Costa Mesa, California 92626-7689
Telephone: (714) 427-7420
Facsimile: (714) 427-7799